BEZPEČNOSTNÝ BULLETIN

Týždeň 07. 07. 2021 - 13. 07. 2021

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Johnson Controls Facility Explorer - bezpečnostná zraniteľnosť	Vysoká	**8.8**
02.	Sensormatic Electronics C-CURE 9000 - bezpečnostná zraniteľnosť	Vysoká	**8.8**
03.	Rockwell Automation MicroLogix 1100 produkt - bezpečnostná zraniteľnosť	Vysoká	**8.6**
04.	Delta Electronics DOPSoft - dve bezpečnostné zraniteľnosti	Vysoká	**7.8**
05.	B&R Industrial Automation produkty - dve bezpečnostné zraniteľnosti	Vysoká	**7.5**
06.	Bachmann Electronic M-Base Controllers - bezpečnostná zraniteľnosť	Vysoká	**7.2**

Národný bezpečnostný úrad
Budatínska 30
851 06 Bratislava

Mail: sk-cert@nbu.gov.sk
Mobil: +421 903 993 706
Tel: +421 2 6869 2915

SK-CERT
Naša značka:
01439/2020/SK-CERT-475

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.8**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Johnson Controls Facility Explorer - bezpečnostná zraniteľnosť

Popis

Spoločnosť Johnson Controls vydala bezpečnostnú aktualizáciu na svoj produkt Facility Explorer, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zasielania špeciálne upravených paketov, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

01.07.2021

CVE

CVE-2021-27661

Zasiahnuté systémy

Facility Explorer vo verzii staršej ako F4-SNC

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-21-182-01

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.8**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Sensormatic Electronics C-CURE 9000 - bezpečnostná zraniteľnosť

Popis

Spoločnosť Sensormatic Electronics vydala bezpečnostnú aktualizáciu na svoj produkt C-CURE 9000, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zasielania špeciálne upravených paketov, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

01.07.2021

CVE

CVE-2021-27660

Zasiahnuté systémy

C-CURE 9000 vo verzii staršej ako 2.80

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-21-182-02
https://www.johnsoncontrols.com/cyber-solutions/security-advisories

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.6**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Rockwell Automation MicroLogix 1100 produkt - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu Rockwell Automation MicroLogix 1100.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených príkazov, spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

08.07.2021

CVE

CVE-2021-33012

Zasiahnuté systémy

MicroLogix 1100 všetky verzie

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame migrovať na novší produkt Micro870.
Administrátorom odporúčame filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry.
Výrobca odporúča blokovať alebo obmedziť všetku komunikáciu TCP/UDP na portoch 2222 a 44818.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-21-189-01

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.8
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Delta Electronics DOPSoft - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Delta Electronics vydala bezpečnostnú aktualizáciu na svoj produkt DOPSoft, ktorá opravuje dve bezpečnostné zraniteľnosti.

Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

01.07.2021

CVE

CVE-2021-27412, CVE-2021-27455

Zasiahnuté systémy

DOPSoft vo verzii staršej ako 4.0.10.18

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).

Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-21-182-03
https://downloadcenter.deltaww.com/en-US/DownloadCenter?v=1&CID=06&itemID=060302&dataType=8&sort_expr=cdate&sort_dir=DESC

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.5
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

B&R Industrial Automation produkty - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť B&R Industrial Automation vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej požiadavky, spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

05.07.2021

CVE

CVE-2021-20986, CVE-2021-20987

Zasiahnuté systémy

X20IF10D3-1 vo verzii staršej ako 1.5.0.0
X20cIF10D3-1 vo verzii staršej ako 1.5.0.0
X20IF10E3-1 vo verzii staršej ako 1.8.0.0
X20cIF10E3-1 vo verzii staršej ako 1.8.0.0
5ACPCI.XPNS-00 vo verzii staršej ako 1.8.0.0

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://www.br-automation.com/downloads_br_productcatalogue/assets/1622986485562-en-original-1.0.pdf
https://www.br-automation.com/downloads_br_productcatalogue/assets/1622986485635-en-original-1.0.pdf

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.2
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Bachmann Electronic M-Base Controllers - bezpečnostná zraniteľnosť

Popis

Spoločnosť Bachmann Electronic vydala bezpečnostnú aktualizáciu na svoje portfólio produktov, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom útoku hrubou silou dešifrovať hash hesiel a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

01.07.2021

CVE

CVE-2020-16231

Zasiahnuté systémy

MX207 vo verzii staršej ako 4.49-P1
MX213 vo verzii staršej ako 4.49-P1
MX220 vo verzii staršej ako 4.49-P1
MC206 vo verzii staršej ako 4.49-P1
MC212 vo verzii staršej ako 4.49-P1
MC220 vo verzii staršej ako 4.49-P1
MH230 vo verzii staršej ako 4.49-P1
MC205 (všetky verzie - ukončená podpora)
MC210 (všetky verzie - ukončená podpora)
MH212 (všetky verzie - ukončená podpora)
ME203 (všetky verzie - ukončená podpora)
CS200 (všetky verzie - ukončená podpora)
MP213 (všetky verzie - ukončená podpora)
MP226 (všetky verzie - ukončená podpora)
MPC240 (všetky verzie - ukončená podpora)
MPC265 (všetky verzie - ukončená podpora)
MPC270 (všetky verzie - ukončená podpora)
MPC293 (všetky verzie - ukončená podpora)
MPE270 (všetky verzie - ukončená podpora)
PC210 (všetky verzie - ukončená podpora)

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania
Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov. Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč. Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje
https://us-cert.cisa.gov/ics/advisories/icsa-21-026-02